Some Help With

# Protecting Your Systems from AvosLocker Ransomware: How AnyDesk Can Help Safeguard Your Data

TABLE OF CONTENT


1. Access Control and Permissions
2. Authentication and Authorization
3. Access Control List (ACL)
4. Session Permission Profiles
5. Disabling Unnecessary Functions
6. Monitoring and Auditing

Additional Prevention Measures Against Ransomware Attacks


AvosLocker ransomware, like many other ransomware variants, exploits vulnerabilities in systems to encrypt files and demand a ransom. One tactic employed by attackers to evade detection and enhance the effectiveness of their attacks is the use of **safe mode** on infected machines. In safe mode, operating systems load only essential services, which may allow attackers to bypass certain security measures and make changes to the system more easily.

As a remote access tool, **AnyDesk** takes significant steps to minimize the risks associated with safe mode usage, helping to safeguard systems against attacks like AvosLocker ransomware. While AnyDesk does not directly prevent the initiation of safe mode, it incorporates various security features designed to mitigate the associated risks:

## 1. Access Control and Permissions

AnyDesk allows administrators to configure specific permissions for remote sessions. Administrators can restrict actions that remote users can take during a session, limiting the attackers' ability to make critical changes to the system, even if they gain access during a ransomware attack.

 © 2026 www.some

### 2. Authentication and Authorization

AnyDesk supports two-factor authentication (2FA) for unattended sessions. This additional layer of security requires the remote user to provide a supplemental security code, thereby reducing the risk of unauthorized access—an essential measure for preventing ransomware from spreading if an attacker gains access to the system.

### 3. Access Control List (ACL)

Utilizing the Access Control List (ACL), administrators can restrict remote connections exclusively to specific clients. This ensures that only authorized devices can connect, minimizing the risk of an attacker leveraging AnyDesk to disseminate ransomware across the network.

### 4. Session Permission Profiles

AnyDesk enables the creation of permission profiles, limiting what the remote user can do during a session. For instance, permissions can be configured to restrict access to certain system areas or disable features such as file transfer, which can help prevent an attacker from using remote access to encrypt files.

### 5. Disabling Unnecessary Functions

Administrators can customize AnyDesk clients to disable features that are not essential for remote support. This includes disabling options that could be exploited by an attacker to move laterally through the network or execute malicious actions.

### 6. Monitoring and Auditing

AnyDesk provides tools for auditing and logging all remote access sessions. These logs can be reviewed to detect unusual or suspicious activities, enabling administrators to identify potential attack attempts and respond swiftly.

## Additional Prevention Measures Against Ransomware Attacks

In addition to the specific features of AnyDesk, it’s crucial to implement supplemental cybersecurity practices to protect against ransomware attacks like AvosLocker:

- **Regular Updates**: Keep all systems and applications up to date to patch known vulnerabilities.
- **Antivirus Software**: Use antivirus and anti-malware software to detect and block threats.

 © 2026 www.some

- **Regular Backups**: Conduct regular backups of important data to facilitate recovery in the event of an attack.
- **Security Awareness Training**: Educate employees about best security practices and how to identify suspicious emails and links.

By leveraging the features of AnyDesk alongside these essential cybersecurity practices, organizations can significantly enhance their defenses against ransomware attacks like AvosLocker.

 © 2026 www.some